01net
OK
nos newsletters
nos magazines
01net Lisez 01net pour 2,45 € / n° seulement

Des milliers de LiveBox Orange piratées par un détournement de DNS

Un mystérieux pirate a réussi à siphonner les données bancaires de milliers de clients de l'opérateur historique en pénétrant l'interface d'administration des Livebox.

Damien Bancal | 01net | le 22/07/14 à 12h06 | laisser un avis

Tweet

agrandir la photo

Que s'est-il vraiment passé fin mai, dans plusieurs milliers de LiveBox Orange ? Subitement, de nombreux internautes se sont retrouvés dans l'impossibilité de se connecter à l'administration de leur box (par l'adresse 192.168.1.1). Le mot de passe permettant d'accéder à leur interface de paramétrage, par laquelle on gère la connexion, le Wi-Fi, ou encore de la télévision avait été changé par un inconnu. Plus grave, l'intrus avait modifié les adresses DNS de la LiveBox et dirigé les connexions des internautes vers un serveur malveillant. Sa mission ? Intercepter les données sensibles des personnes piégées. Une attaque dite Man-in-the-middle (L'homme du milieu). « *Tous les flux vers des sites marchands, les banques ont été redirigés vers le fraudeur* » s'exclame un responsable d'un service de sécurité informatique bancaire contacté par 01net.

Seule alerte que les clients ont éventuellement pu apercevoir : l'apparition d'un problème de certificat lors de leurs achats en ligne. Autant dire que l'attaque, sournoise, a peut-être fait de gros dégâts, le pirate ayant eu la possibilité de capturer les coordonnées bancaires, les identifiants de connexion, voire leurs coordonnées e-CB sans que les victimes ne puissent s'en rendre compte.

Comment ce cybercriminel a-t-il fait pour se prendre ainsi aux box de milliers d'internautes ? Il semble avoir réussi son tour de passe-passe par le biais d'un site piégé. L'idée était de faire exécuter un script malveillant spécifiquement aux clients Orange grâce à un lien attirant, formulé à leur égard. Celui-ci lançait alors un script automatisé qui se connectait à l'interface d'administration de la LiveBox.

Mise à jour salvatrice pour les Livebox

Le cybercriminel a aussi profité du fait que les clients impactés n'avaient pas changé leurs identifiants de connexion «Usine» de leur LiveBox, le fameux admin/admin. Une attaque facile ? Des codes trainent sur le web permettant, en quelques lignes, de se connecter automatiquement à une LiveBox, de modifier le DNS et de changer le mot de passe. Autant dire un jeu d'enfant pour un pirate.

Contacté, Orange n'a pas donné suite à nos questions sur cette attaque... mais semble l'avoir prise au sérieux : depuis, l'opérateur a mis à jour ses LiveBox qui, dorénavant, n'autorisent plus les changements de DNS. *« Je travaille dans une banque et j'en ai ras le bol de traiter des incidents de ce type »* souligne le RSSI joint par 01net. *On se fait taper dessus par nos clients en leur renouvelant leur CB par mesures préventives. Il serait bien que chacun prenne ses responsabilités…* » Il est vrai qu'Orange est loin d'être le seul à avoir subi ce genre d'attaques, qui sont fréquentes chez tous les FAI. Alors, pour vous éviter toute mésaventures, suivez notre petit guide, ci-dessous.

@01net sur twitter

à lire aussi
SUR LES MÊMES THÈMES

- Amazon au service de la CIA et de la NSA
- Cartes bancaires : 20 fois plus de fraudes sur Internet qu'en magasin
- L'édifiant arsenal des espions britanniques pour manipuler les contenus sur le Web
- Projet Zero : Google ouvre la chasse aux failles zero day avec une unité d'élite
- CNET.com hacké pour sensibiliser le web aux questions de sécurité ?
- Smartphone d'occasion : vous vendez vos données personnelles sans le savoir
- Silent Circle lance des forfaits de voix sur IP chiffrée
- La base de données des fonctionnaires américains, piratée depuis la Chine
- Des données personnelles de membres du site l'Equipe.fr dans la nature
- La NSA a espionné d'éminents musulmans américains
- Invisible.im, la messagerie instantanée qui ne veut laisser aucune trace
- Vols vers les Etats-Unis : quels risques posent réellement les terminaux mobiles?
- La NSA récolte avant tout des données de vie privée de gens ordinaires
- Fuites de la NSA : y a-t-il un second Edward Snowden ?
- Des hackers et des FAI portent plainte contre les services secrets britanniques
- Pour la NSA, les utilisateurs de Tor ou Tails Linux sont des «extrémistes»
- Plus de 100 personnes ont été arrêtées grâce à la surveillance du Net par la NSA
- Quand Microsoft fait tomber des millions de sites web pour s'attaquer à un botnet
- Le rapport sur la cybercriminalité alerte les défenseurs des libertés citoyennes

Comment vous prémunir de ce genre d'attaques ?

Pour éviter ce type de piège automatisé, quelques règles d'hygiène numérique simples sont à tenir. D'abord, changer les mots de passe usine de votre LiveBox (mais aussi de votre téléphone, tablette...) Pour Orange, SFR il suffit de taper **192.168.1.1** dans un navigateur.Pour Numéricâble, **192.168.0.1.** Pour Freebox V5 **https://subscribe.free.fr/login/** et V6 **http://mafreebox.freebox.fr/**. Il vous suffit de tester le couple admin/admin pour s'identifier. Si vous accédez à l'administration de la box, direction «**Changer de mot de passe**».

Dernier détail, ne cliquez jamais sur le moindre lien vous proposant de vous rendre dans votre administration de box. Préférez toujours taper l'adresse dans votre navigateur. Cela pourra vous éviter le passage d'un pirate !

envoyer par mail
imprimer l'article
Tweet
Suivre @01net

Actu précédente
Amazon au service de la CIA et de la NSA

01net
CGV - Conditions d'abonnement - Charte de confiance - Recrutement - Contacts - Mentions légales et CGU
NextInteractiveMedia : 01net - RMC - RMC SPORT - RMC DÉCOUVERTE - BFMTV - BFM BUSINESS - 01Business - Association RMC/BFM
lecharger.com OK GUIDE D'ACHAT ASTUCES